Security Architecture and Design Documentation Guidance

SECURITY PROBLEM

Version 2.5

Prepared by HR CDS TT

23 June 2011

REVISION HISTORY

Name	Date	Reason For Changes	Version
HR CDS TT	11 October 2010	Document creation	1.0
HR CDS TT	19 October 2010	Group review and modification	2.0
HR CDS TT	20 October 2010	Threats as assumptions	2.1
HR CDS TT	21 October 2010	Group review and modifications	2.2
HR CDS TT	13 January 2011	Removed reference to formality	2.3
HR CDS TT	3 March 2011	Review and update by Tiger Team	2.4
HR CDS TT	23 June 2011	Update by Tiger Team	2.5

ACRONYMS AND DEFINITIONS

Acronym	Definition
CCA	Covert Channel Analysis
CDS	Cross Domain Solution
DRD	Development Representation Documentation
DTLS	Descriptive Top-Level Specification
FTLS	Formal Top-Level Specification
HLD	High Level Design
LLD	Low Level Design
SFS	Security Functional Specification
SP	Security Policy

INTRODUCTION

The precise, deterministic and logical statement(s) that defines the nature and scope of the security protections necessary for mission accomplishment. This statement addresses the assumptions of the solution's operational environment (physical security, personnel security, procedural security, and operational capabilities), the security policy (derived from the mission objectives) the solution enforces, and threats that the solution in combination with operational environment counters. There are assumptions made about mission environment, which when combined with the internal properties of the solution should satisfy the security assertions and subsequently the mission requirements. Security Objectives are derived from the Security Problem. All these interactions are summarized in Figure 1, which also shows the relationship of the Security Problem to the other topic areas described in the DRD.

The evaluation should validate that the solution behaves according to these assumptions and assertions.

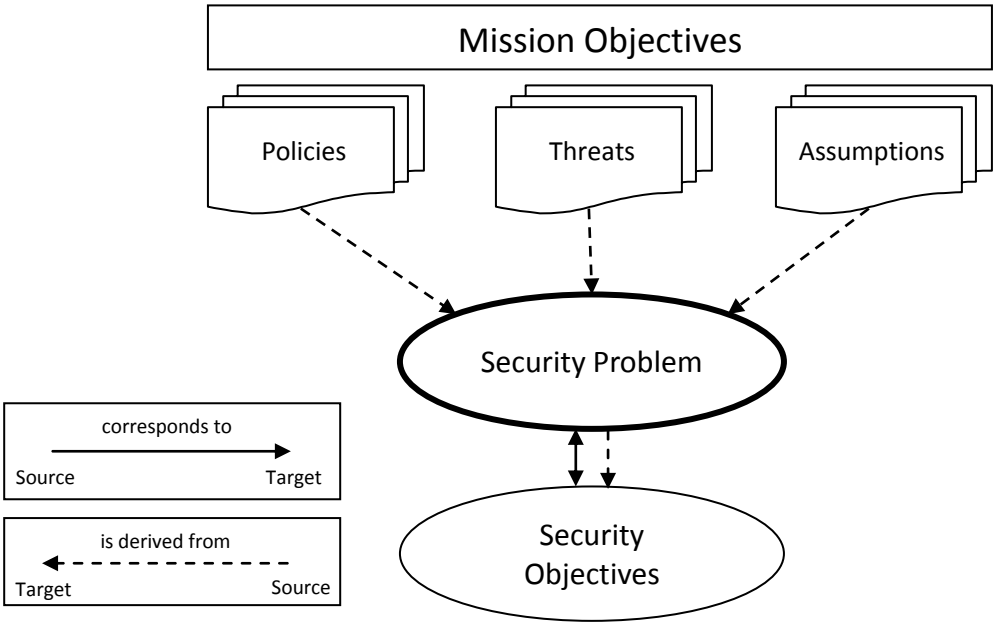

Figure 1 - Security Problem Interactions

ASSUMPTIONS

There are three categories of assumptions. There are those assumptions regarding the mission's operational environment and those regarding the data. The threats are in fact another level of assumptions. Threats are potential events, which may result in violation of the solution's security policy or exercise a lack of comprehensiveness[1] in the solution's security policy.

[1] A threat that exercises a lack of comprehensiveness in the solution's security policy is exploiting an aspect that was not described by the solution's security policy.

OPERATIONAL ENVIRONMENT

There are assumptions that are made regarding the operational environment external to the solution, which may support security functionality. These assumptions fall into the following categories:

Physical Aspects of Operational Environment – Assume minimizations of electromagnetic emanations by the solution, network separation, and that the solution is located in a physically restricted access area.

Personnel Aspects of Operational Environment – Assume that users will be sufficiently cleared to access the information contained within the solution and trained in the use of the solution, as well as basic information security.

Connectivity Aspects of Operational Environment – Assume the solution may be connected to one or more networks of unknown trustworthiness.

DATA

There are assumptions made regarding the data and these assumptions fall into the following categories:

Properties(s) – Assumptions might include origin, age, CIA of data as generated by source, CIA of communications channels between source and destination, and relationships with other participants.

Protocol(s) – Assumptions might include data structures, sequencing, timing of bits and the solution's interpretation of the bits.

THREATS

The known threats should be considered. The solution security policy should identify the known threats that will be addressed.

CNSSI No. 4009 defines threat as:

> *"Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service."*

SECURITY POLICY

Security policies are based on laws, regulations, rules, procedures, and guidelines that are required by the mission or the organization(s) controlling the mission's operational environment. The solution's security policy is the interpretation of those policies relevant to the mission. The mission security policy will be enforced by a combination of the assumptions above and the intended implementation of the solution. The evaluator(s) should validate that the solution behaves according these policies.